



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 3820.3F
DUSN
2 Jan 2020

SECNAV INSTRUCTION 3820.3F

From: Secretary of the Navy

Subj: INTELLIGENCE OVERSIGHT WITHIN THE DEPARTMENT OF THE NAVY

Ref: (a) DoD Directive 5148.11 of 24 April 2013
(b) DoD Directive 5148.13 of 26 April 2017
(c) E.O. 12333 as amended
(d) DoD Directive 5240.01 of 22 March 2019
(e) DoDM 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities of 8 August 2016
(f) DOD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons," Incorporating Change 2, effective 26 April 2017
(g) SECNAVINST 5000.34F
(h) Presidential Policy Directive 19 of 10 October 2012
(i) Memorandum of Understanding Between the Department of Defense and Department of Justice, "Reporting of Information Concerning Federal Crimes," of 22 August 1995
(j) National System for Geospatial Intelligence Manuals (NSGM) FA 1806 of March 2019
(k) UNSECNAV Memo, "Definition of Intelligence Related Activities" of 17 September 20s18
(l) MCO 3800.2B
(m) SECNAV M-5214.1

Encl: (1) Definitions
(2) Responsibilities
(3) Quarterly Intelligence Oversight Report Format Template
(4) Intelligence Oversight Inspection Checklist

1. Purpose

a. To implement policies, procedures, and governing regulations regarding the conduct of intelligence and intelligence-related activities and a system of program reviews, inspections, and reporting requirements for intelligence oversight activities within the Department of the Navy (DON).

2 Jan 2020

b. This instruction has been substantially revised and should be reviewed in its entirety.

c. Enclosures (1) through (4) provide definitions, responsibilities, a quarterly intelligence oversight report format template, and intelligence oversight inspection checklist, respectively.

2. Cancellation. SECNAVINST 3820.3E.

3. Definitions. See Enclosure (1).

4. Applicability

a. This instruction applies to the Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), and the Commandant of the Marine Corps (CMC), and all U.S. Navy (USN) and U.S. Marine Corps (USMC) installations, commands, activities, field offices, and all other organizational entities within the DON. It applies to all personnel, consultants, and supporting contractors when contract performance includes any intelligence activities or intelligence-related activities.

b. No program or activity shall be exempt from the requirements of this instruction, regardless of sensitivity, classification, compartmentalization, or degree of restriction on access.

c. This instruction applies to the Naval Criminal Investigative Service (NCIS) in its role as a Defense Intelligence Component. It applies to the conduct of intelligence and intelligence-related activities by the NCIS, but not the conduct of criminal or law enforcement investigations or other law enforcement activities.

d. Nothing in this issuance will be construed to preclude, supersede, or limit the existing authorities and policies governing reporting of criminal or counterintelligence matters to the Defense Criminal Investigative Organizations (DCIO) and Military Department Counterintelligence Organizations (MDCO). NCIS is the DON DCIO and MDCO.

2 Jan 2020

5. Policy

a. DON components and department elements, their personnel, and supporting contractors and consultants shall carry out their authorized intelligence and intelligence-related activities in strict conformity with the U.S. Constitution, applicable laws, Executive Orders (E.O.), and other relevant directives, including the intelligence and Intelligence Oversight (IO) directives specified in references (a) through (m), and this instruction.

b. Special emphasis shall be given to the protection of the constitutional rights and privacy of U.S. Persons. The collection, retention, and dissemination of U.S. Person Information (USPI), when conducted as an intelligence activity, is governed by the requirements set forth in reference (e). Note that intelligence and intelligence-related activities covered by this instruction are not limited to those that concern U.S. Persons.

c. An activity or conduct that qualifies as either a Questionable Intelligence Activity (QIA) or a Significant or Highly Sensitive Matter (S/HSM) is reportable without waiting for substantiation, completion of an investigation, formal adjudication, or final resolution of the issue.

d. Per references (b) and (h), no adverse action will be taken against any Department of Defense (DoD) personnel because they intend to report to appropriate authorities what they reasonably believe is a QIA or S/HSM. Similarly, no adverse action will be taken against DoD contractor personnel because they intend to report to the appropriate authorities what they reasonably believe is a QIA or S/HSM.

e. Nothing in this instruction is intended to exempt DON components and department elements conducting intelligence and intelligence-related activities from complying with any separate non-IO related reporting requirement.

f. Nothing in this instruction is intended to exempt DON components or personnel from adhering to the enhanced security requirements and policies for special access programs (SAP). The Director, DON Special Access Program Central Office (SAPCO) will coordinate all SAP-related QIA, S/HSM, or Quarterly Reports

2 Jan 2020

to ensure appropriate access, notification, and coordination processes are executed in support of the DON IO official.

g. This instruction is not a source of authority for the conduct of intelligence or intelligence-related activities.

6. Responsibilities. See Enclosure (2).

7. Quarterly IO Report Format Template. See Enclosure (3).

8. IO Inspection Checklist. See Enclosure (4).

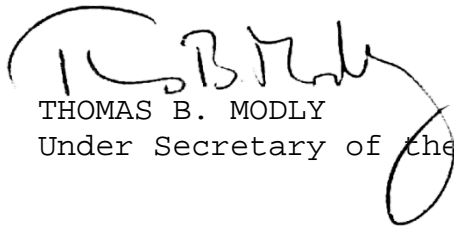
9. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page:

<https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx>.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office.

10. Information Management Control. The reporting requirement contained in paragraphs 7b, 8c, 9(b), and (f) of enclosure (2) are exempt from information collection control, per reference (m), Part IV, paragraph 7(i).



THOMAS B. MODLY
Under Secretary of the Navy

Distribution:

Electronic only, via Department of the Navy Issuances website

<https://www.secnav.navy.mil/doni/>.

DEFINITIONS

1. Counterintelligence. Per reference (c), information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities.

2. Foreign Intelligence. Per reference (c), information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists.

3. Intelligence Activities. All activities that DoD Components conduct pursuant to reference (c).

4. IO. The process of independently ensuring all DoD intelligence and intelligence-related activities are conducted in accordance with applicable U.S. law, E.O.'s, Presidential Directives, Intelligence Community Directives, and DoD issuances designed to balance the requirements for acquisition of essential information by the Intelligence Community, and the protection of U.S. Constitutional and Statutory Rights of U.S. Persons. IO also includes the identification, investigation, and reporting of QIAs and S/HSMs involving intelligence or intelligence-related activities.

5. Intelligence-Related Activities. Per reference (k), activities that are not conducted under the authority of reference (c) that involves the collection, retention, or analysis of information, and the activities' primary purpose is to:

a. Train intelligence personnel.

b. Conduct research, development, or testing and evaluation for the purpose of developing intelligence-specific capabilities. Activities that use intelligence funding (e.g., Military Intelligence Program or National Intelligence Program) are presumed to be intelligence or intelligence-related activities.

Specifically excluded from this definition are operational security activities, such as own force monitoring, force protection, maintenance of technologies or systems, cyberspace surveillance and reconnaissance operations, and activities listed in reference (e) Section 3.1.a.(3) along with all research, development, testing, evaluation, and training activities conducted in support of those activities. This is not an exhaustive list.

6. QIA. Per reference (b), any intelligence or intelligence-related activity when there is reason to believe such activity may be unlawful or contrary to an E.O., Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity.

7. Shared Repository. A database, environment, or other repository maintained for the use of more than one entity. A database, environment, or other repository that a contractor or other entity maintains for the use of a single Defense Intelligence Component, or those acting on its behalf, is not a shared repository.

8. S/HSM. Per reference (b), an intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an E.O., Presidential Directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential:

- a. Congressional inquiries or investigations.
- b. Adverse media coverage.
- c. Impact on foreign relations or foreign partners.
- d. Systemic compromise, loss, or unauthorized disclosure of protected information.

RESPONSIBILITIES

1. The SECNAV is responsible to the Secretary of Defense for all matters within the DON, which includes the effective supervision, oversight, and control of intelligence activities, intelligence-related activities, sensitive activities, and SAPs per reference (g).
2. The Under Secretary of the Navy (UNSECNAV) is responsible for providing oversight and management of all intelligence activities, intelligence-related activities, and SAPs within the DON.
3. The Deputy Under Secretary of the Navy (DUSN) is responsible for:
 - a. Advising the UNSECNAV regarding the oversight of activities covered by this instruction.
 - b. Ensuring coordination and assisting UNSECNAV with IO responsibilities.
4. The CNO and the CMC are responsible for:
 - a. Implementing the policies and procedures contained in references (a) through (g), and this instruction.
 - b. Appointing an Intelligence Oversight Officer (IOO) of appropriate grade and intelligence experience commensurate with their oversight responsibilities, who has the necessary clearance and is eligible for access to all organization intelligence and intelligence-related activities (including those protected by SAP, Alternative Compensatory Control Measures (ACCM), and other security compartments).
 - c. Ensure that each appointed IOO provide a Service/Component consolidated Quarterly IO report to the DON IO Official using the format in enclosure (3).
 - d. Ensuring the General Counsel of the Navy (GC), Naval Inspector General (NAVIG), the Judge Advocate General of the Navy (JAG), the Staff Judge Advocate to the CMC (SJA to CMC), and the Deputy Naval Inspector General for Marine Corps Matters

(DNIGMC) have access to information necessary to carry out their duties under this instruction.

5. The Director, NCIS is responsible for:

a. Implementing the policies and procedures contained in references (a) through (g), and this instruction.

b. Appointing an IOO of appropriate grade and intelligence experience commensurate with their oversight responsibilities, who has the necessary clearance and is eligible for access to all organization intelligence and intelligence-related activities (including those protected by SAP, ACCM, and other security compartments).

c. Ensure that the appointed IOO provide a consolidated Quarterly IO report to the DON IO Official using the format in enclosure (3).

d. Ensuring the GC, NAVIG, and JAG have access to information necessary to carry out their duties under this instruction.

6. The GC, in coordination with the JAG and/or the SJA to CMC, is responsible for:

a. Ensuring all intelligence and intelligence-related activities are conducted in a legal manner, per references (a) through (k).

b. Review results of all QIA or S/HSM investigations to determine whether the activity is legal and consistent with applicable policy, per reference (b).

7. The Senior Director for Security and Intelligence, under the direction and control of the DUSN, is responsible for:

a. Serving as the DON IO Official and administering the DON IO Program in accordance with reference (b).

b. Reviewing, consolidating, and submitting all DON S/HSMs, QIAs, and Quarterly IO Reports to the DoD Senior Intelligence Oversight Official (SIOO) per reference (b). Coordinate with DON SAPCO on submission of reports requiring SAP protection.

c. Serving as the DON point of contact for DoD SIOO IO inspections of DON organizations.

8. The NAVIG and DNIGMC are responsible for:

a. Per reference (b), inspecting the DON component and the department elements to ensure compliance with references (a) through (g).

b. Investigating reported QIAs or S/HSMS to the extent necessary to determine the facts and to assess whether the activity is consistent with applicable policies per reference (b). Suspected criminal activities will be referred to NCIS for investigation per reference (i).

c. NAVIG and DNIGMC will provide a Quarterly IO report to the DON IO Official using the format in enclosure (3). Coordinate with DON SAPCO on submission of reports requiring SAP protection.

d. Maintaining a cadre of appropriately cleared and qualified personnel to conduct reviews, inspections, and investigations. NAVIG and DNIGMC will discharge these responsibilities, in part, through their inspection program and their staffs' participation in the Senior Review Board, Sensitive Activities Oversight Committee, Special Programs Review Group, and Sensitive Activities Review Group, per reference (g).

9. The Heads of DON organizations, including SYSTEMS COMMAND (SYSCOMS), Program Executive Officers, and Heads of Naval Academic Institutions, that conduct intelligence or intelligence-related activities are responsible for:

a. Appointing an IOO who is of appropriate grade and intelligence experience commensurate with their oversight responsibilities, who has the necessary clearance and is eligible for access to all organization intelligence and intelligence-related activities (including those protected by SAP, ACCM, and other security controls).

b. Establishing processes and procedures for the periodic comprehensive review of all intelligence and intelligence-related activities under the organization's authority, direction, and control to verify compliance with federal law,

E.O.'s, Presidential Directives, Intelligence Community Directives, and DoD and SECNAV issuances. Reviews of inspection reports generated by the cognizant Inspector General (IG), pursuant to the requirements set forth below in section (g) of the enclosures, meet this requirement.

c. Ensuring that a legal review is conducted prior to commencing activity whenever a reasonable person would believe that the intelligence or intelligence-related activity may be contrary to federal law, E.O.'s, Presidential Directives, Intelligence Community Directives, and DoD issuances.

d. Administering an IO training program that is tailored to mission requirements and provides initial and annual refresher IO training to all employees involved in intelligence and intelligence-related activities. At a minimum, training will include:

(1) Familiarity with the authorities and restrictions established in reference (d), (e), and other applicable Intelligence Community Directives and DoD issuances governing applicable intelligence and intelligence-related activities.

(2) Responsibilities of DoD personnel and DoD contractor personnel for reporting QIAs and S/HSMs in accordance with reference (b).

e. Periodically review command produced intelligence and intelligence-related products for compliance with references (c) through (f).

f. Submitting S/HSM, QIA, and Quarterly IO report to the DON IO Official using the format in enclosure (3). Coordinate with DON SAPCO on submission of reports requiring SAP protection.

(1) S/HSM will be submitted immediately.

(2) QIA will be submitted quarterly as part of the Quarterly IO Report.

(3) The Quarterly IO Report is due to the DON IO Official five calendar days after the end of each quarter. Quarterly IO reports are based on calendar year.

(4) Component Commands working under Combatant Command authorities will also provide a copy of the Quarterly IO Report to the DON IO Official.

(5) Organizations may consolidate report inputs from subordinate commands and provide a single Quarterly IO Report to the DON IO Official for incorporation into subsequent reporting to DoD SIOO.

g. Ensuring that the cognizant command IG inspects all elements of the organization involved in intelligence and intelligence-related activities at an interval of no greater than once every 36 months, with appropriate follow-up or assistance between inspections as deemed necessary. Ensure that when completed, the 36 month cycle results in a comprehensive review of all intelligence and intelligence-related activities under the organization's authority, direction, and control to verify compliance with all applicable federal law, E.O.'s, Presidential Directives, Intelligence Community Directives, DoD Issuances, and DON Issuances. Ensure that these inspections include a review of intelligence products produced by the organization for compliance with applicable standards. Enclosure (4) will be used as a baseline checklist during inspections of Secretariat-level and Navy commands. Marine Corps commands will refer to reference (1), as amended, for checklist guidance.

h. Ensuring the cognizant command IG investigates each QIA or S/HSM to the extent necessary to determine the facts and to assess whether the activity is consistent with applicable policies per reference (b). Marine Corps commands will coordinate QIA or S/HSM investigations with DNIGMC. Suspected criminal activities will be referred to NCIS for investigation per reference (i).

i. Reporting to NCIS any possible violation of federal criminal law by an employee or a possible violation of specified federal criminal laws by any other person, as required in reference (i).

j. Providing access to all intelligence and intelligence-related activities to appropriately cleared IG and legal representatives conducting IO responsibilities. Ensure employees of their organizations cooperate fully with such officials. Coordinate with DON SAPCO where IO responsibilities may require access to SAP.

k. Ensuring that all subordinate intelligence components, units, and elements in or under their command comply with the requirements of references (a) through (f), and this instruction.

QUARTERLY IO REPORT FORMAT TEMPLATE

3800
Ser/xxxx
dd mmm yy

From: Your Command
To: Senior Director for Security & Intelligence, Deputy Under
Secretary of the Navy

Subj: (U) QUARTERLY INTELLIGENCE OVERSIGHT REPORT - XX QUARTER
CALENDAR YEAR 20XX

Ref: (a) Executive Order 12333, as amended
(b) DoD Directive 5240.01 of 22 March 2019
(c) DoD Directive 5148.13 of 26 April 2017
(d) DoDM 5240.01, "Procedures Governing the Conduct of
DoD Intelligence Activities," of 28 August 2016
(e) DoD 5240.1-R, "Procedures Governing the
Activities of DoD Intelligence Components That Affect
United States Persons," Incorporating Change 2,
effective 26 April 2017
(f) SECNAVINST 3820.3F

1. (U) Per references (a) through (f), this report is submitted
for the period of dd month yyyy to dd month yyyy.

2. (U) New Incidents: For example, there are two new incidents
to report; all are Questionable Intelligence Activities (QIA)).
(U) File Number: enter your command case #. Each case # should
end in either a "Q" or a "S" to indicate whether the case is a
QIA or a S/HSM. For example, "NAV-2017-01-Q."

(1) (U) Incident Description: the incident description
section should be able to stand on its own and include who,
what, when, and whether any allegations are substantiated, not
substantiated, or under investigation.

(2) (U) Timeline:

(a) (U) Occurred: dd month yyyy. For example, "12
January 2018" - or - "November 2017 to February 2018."

(b) (U) Discovered: dd month yyyy. For example, "15 February 2018".

(c) (U) Reported to the Naval Inspector General (NAVINSGEN): For example, this report - or - 23 August 2017 via memorandum for the record, phone, email, etc.

(3) (U) Reason for Report: For example, QIA, in violation of reference (d) Para 3.3.c.2 and Para 3.3.f.2.

(4) (U) Cause: Indicate why the incident occurred. If still under investigation, "Pending investigation" is an acceptable answer.

(5) (U) Impact on National Security or International Relations: none, to be determined, yes, likely, or no impact is anticipated. For yes or likely answers, include a brief explanation of how incident will impact national security or international relations.

(6) (U) Impact on Civil Liberties or Privacy: none, to be determined, yes, likely, or no impact is anticipated. For yes or likely answers, include a brief explanation of how incident will impact civil liberties or privacy. For example, "Yes, USPI was collected without proper authorities and improperly retained."

(7) (U) Remedial Action: An explanation of action taken or planned to prevent recurrence of the incident.

(8) (U) Additional Information: Any additional information not already reported that you considered relevant for purposes of fully informing Senior Leadership about the incident. If none then mark the section "None."

(9) (U) Status: Indicate whether the incident is open or closed. If open, provide the status of the ongoing investigation. If closed, include a notation indicating whether any allegations were substantiated or not substantiated. For example, "closed, substantiated" - or - "Open, investigation was formally commenced by NAVINSGEN on 10 April 2018 and assigned by the NAVINSGEN Tracking System case #12345."

3. (U) Updates on Previously Reported Incidents: Use the same format as Section 2 for previously reported incidents still under investigation as well as those resolved and closed during the quarter. The update should contain enough information that the report can stand on its own without reading original report.

4. (U) Crimes Reported: Provide a narrative summary of any intelligence or intelligence-related activity that has been or will be reported to the U.S. Attorney General, or that must be reported to the U.S. Attorney General as required by law or other directive, including crimes required by reference (a) to be reported to the U.S. Attorney General. If none then mark the section "None."

5. (U) Trend Reporting: Identify and explain common causal factors for QIAs and S/HSMs. Include supporting data and metrics supporting the analysis. If none then mark the section "None."

6. (U) Significant Inspection Findings or IO Program Developments: Provide a description of any significant internal inspection findings or IO program developments (e.g. training initiatives, awareness, indoctrination, familiarization, published documents, new instructions, or policy). Examples of significant inspections findings are: "A DoD IO computer based training module would greatly improve DON's ability to provide standardized training by addressing the IO core concepts from the DoD-wide perspective. This baseline training would also serve as a common launching point for commands to build supplemental IO training and keep them aligned with wider DoD goals, lessons learned, and best practices." Include a summary of any IO training conducted in the previous quarter. If none then mark the section "None."

7. (U) IO Inspections Conduct This Quarter: Identify any subordinate commands that were inspected during the quarter in the following format.

SECNAVINST 3820.3F
2 Jan 2020

COMMAND

INSPECTION DATE

Command Alpha

dd month yyyy

Command Bravo Detachment ONE

dd month yyyy

8. (U) IO POC is xxxxx, rank and job title, (xxx)xxx-xxxx,
firstname.lastname@navy.mil.

NAME OF SIGNED

IO INSPECTION CHECKLIST

IO INSPECTION CHECKLIST		
Inspected Organization:	Inspector(s):	Date:
<p>References:</p> <p>(a) E.O. 12333, as amended</p> <p>(b) DoD Directive 5240.01 of 22 March 2019</p> <p>(c) DoDM 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," of 8 August 2016</p> <p>(d) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," Incorporating Change 2, effective 26 April 2017</p> <p>(e) DoD Directive 5148.13 of 26 April 2017</p> <p>(f) SECNAVINST 3820.3F, Oversight of Intelligence Activities within the Department of the Navy, dd mmm yyyy</p>		
Part 1: Governance and Management		
1	<p>Does your organization have an IO Instruction, Standards Operating Procedure, or Manual?</p> <p>Remarks:</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
2	<p>Does your organization have a designated IOO Officer?</p> <p>- Is the IOO of appropriate grade and intelligence experience commensurate with their oversight responsibilities who has access to all organization intelligence and intelligence-related activities (including those protected by special access programs, alternative compensatory control measures, and other security compartments) and who has direct access to the organization commanding officer/director/head to report on intelligence oversight compliance?</p> <p>(DoD Directive 5148.13 para 2.4.h and SECNAVINST 3820.3F Enclosure (2) para 5.a</p> <p>Remarks:</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
3	<p>Does your organization have a process for reviewing command intelligence activities and intelligence-related activities under the organization's authority, direction, and control to verify compliance with applicable federal law, E.O.'s, Presidential directives, Intelligence Community Directives, DoD, and SECNAV issuances?</p> <p>- Does the process include a legal review when required, or appropriate?</p> <p>- Is process codified in an instruction or standard operating procedure, etc.?</p> <p>(DoD Directive 5148.13 para 2.4.a and SECNAVINST 3820.3F Enclosure (2) para 5.b</p> <p>Remarks:</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No

	Remarks:
4	<p>Does your organization verify that all contracts involving intelligence or intelligence-related activities or supporting those efforts under DoD authorities requires personnel to report any QIA or S/HSM to appropriate Government officials identified in the contract?</p> <p><i>(DoD Directive 5148.13 para 4.1.e and SECNAVINST 3820.3F Enclosure (2) para 5.i)</i></p> <p>Remarks:</p>
5	<p>Does your organization provide the DON organization legal counsel/SJA, GC/JAG/SJA to CMC, DUSN Intelligence IOO, and any IG of competent jurisdiction with access to any employee and with all information necessary to perform their IO oversight responsibilities, including information protected by SAP, alternative compensatory control measures, or other security compartmentalization? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>- Is the organization IG and legal counsel cleared to all programs/activities?</p> <p><i>(DoD Directive 5148.13 para 2.4.g and SECNAVINST 3820.3F Enclosure (2) para 1.c, para 5.i.or)</i></p> <p>Remarks:</p>
6	<p>Does your organization host or participate in a shared repository (database)? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>- If so, does the shared repository contain USPI?</p> <p>- Is the shared repository with USPI done IAW DoDM 5240.01?</p> <p>- Is there an instruction, SOP or Manual for preventing a violation when storing or accessing the shared repository (database)?</p> <p><i>(DoDM 5240.01 3.1.b)</i></p> <p>Remarks:</p>
Part 2: Reporting	
7	<p>Does your organization have a process to report S/HSM and QIA? <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>- Immediately for S/HSM</p> <p>- Quarterly for QIA</p> <p>- Format in accordance with DoD SIOO and current DON template</p> <p><i>(DoD Directive 5148.13 para 4.1.d, 4.3.a, 4.4.a, 4.4.b, and Figure 1 and SECNAVINST 3820.3F Enclosure (2) para 5.e and Enclosure (3))</i></p> <p>Remarks:</p>

8	<p>Does your organization have a process to report any crimes involving any intelligence activity or intelligence-related activity to NCIS? (DoD Directive 5148.13 para 4.3.a(3) and SECNAVINST 3820.3F Enclosure (2) para 5.h) Remarks:</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
9	<p>Does your organization submit quarterly IO reports?</p> <ul style="list-style-type: none"> - Due no later than 5 calendar days after end of reporting quarter - Format in accordance with template - The Heads of DON organizations, including SYSCOMS, Program Executive Officers, and Heads of Naval Academic Institutions, that conduct intelligence or intelligence-related activities are responsible for submitting S/HSM, QIA, and Quarterly IO report to the DON Intelligence Oversight IO Official using the format in enclosure (3). <p>(DoD Directive 5148.13 para 4.4.b, and Figure 1 and SECNAVINST 3820.3F Enclosure (2) para 5.e , or Enclosure (3)) Remarks:</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
Part 3: Training		
10	<p>Does your organization administer an IO training program that is appropriately tailored to mission requirements (initial and annual refresher)?</p> <ul style="list-style-type: none"> - At a minimum, IO training will include: (1) Familiarity with the authorities and restrictions established in DoDD 5240.01, DoDM 5240.01, and other applicable Intelligence Community Directives and DoD issuances governing applicable intelligence activities. (2) Responsibilities of DoD personnel and DoD contractor personnel for reporting QIAs and S/HSMs <ul style="list-style-type: none"> - What is the process for tracking and documenting? - Does all senior leadership, with cognizance over intelligence or intelligence-related activities, receive IO training? <p>(DoD Directive 5148.13 para 2.4.c and SECNAVINST 3820.3F Enclosure (2) para 5.c) Remarks:</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No
11	<p>Do individuals at the organization understand:</p> <ul style="list-style-type: none"> - What constitutes a S/HSM, QIA, and USPI? - S/HSM and QIA reporting responsibilities (report immediately to their chain of command or supervisor) - Restriction established in DoDD 5240.01 and DoDM 5240.01 <p>(DoD Directive 5148.13 para 2.4.c, 4.1.d and SECNAVINST 3820.3F Enclosure (2) para 5.d) This question is used to determine effectiveness of intelligence oversight training Remarks:</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No

Part 4: Inspections	
12	<p>Does your cognizant Command IG conduct IO inspections on all components, units, and elements in or under your command at an interval of no greater than once every 36 months, with appropriate follow-up/"spot checks" or assistance between inspections as deemed necessary?</p> <p style="text-align: right;"><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><i>(DoD Directive 5148.13 para 4.1.b through d and SECNAVINST 3820.3F Enclosure (2) para 5.f)</i> Remarks:</p>
Part 5: Investigations	
13	<p>Does your cognizant Command IG conduct IO investigations into alleged QIAs and S/HSMs to the extent necessary to determine the facts and to assess whether the activity is legal and consistent with applicable policies?</p> <p style="text-align: right;"><input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>- Investigations will require a written report that includes a description of the incident and a determination of whether the allegation was substantiated. If the allegation is substantiated, does the report will include findings of fact, an assessment of the cause, and recommended remedial action to prevent recurrence?</p> <p>- How are they referred to IG <i>(DoD Directive 5148.13 para 4.2.a through 4.2.d and SECNAVINST 3820.3F Enclosure (2) para 5.g)</i> Remarks:</p>
Additional Notes:	
Inspecting Official (Print Name Title, Phone)	Inspecting Official's Signature